Express Mail Label NO. EL480563848US

OPTICAL SECURITY SYSTEM USING FOURIER PLANE ENCODING

STATEMENT OF GOVERNMENTAL INTEREST

This application was supported by the USAF Rome Lab grant F19628-95-C-0136 and the National Science Foundation.

RELATED APPLICATIONS

This application claims the benefit of U.S. provisional application No. 60/117,872, filed January 29, 1999 which is incorporated herein by reference as if set forth at length.

TECHNICAL FIELD

This invention relates to a system and method for verifying the authenticity of an object utilizing signal processing techniques.

BACKGROUND OF THE INVENTION

Due to the rapid advances in computers, CCD technology, image-processing hardware and software, printer, and copiers, there is an increase potential of fraud by reproducing the patterns and pictures used to verify the authenticity of the objects. The application of optical processing and pattern recognition for security verification of credit cards, passports and other forms of biometrics image identification have been proposed (1. B. Javidi and J.L. Horner, "Optical pattern recognition for validation and security verification," *Opt. Eng.*, ***33***(6), 1752-1756 (1994); H.-Y. Li, Y. Qiao, and D. Psaltis, "optical network for real-time face recognition", *Appl. Opt.* **32**, 5026-5035 (1993);T. Grycewicz, and B. Javidi, "Experimental comparison of binary joint transform correlators used for fingerprint identification," *Opt. Eng.*, **35**(9), 2519-2525 (1996); P.K.H. Fielding,

J.L. Horner and C.K. Makekau, "Optical fingerprint identification by binary joint transform correlation," *Opt. Eng.*, **30**(12), 1958-1961 (1991); C.L. Wilson, C.I. Watson, E.G. Pack, "Combined optical and neural network fingerprint matching" in Optical Patteern Recognition VIII, D.P. Casasent and T. Chao, ed., Proc. Soc. Photo-Opt.Instrum. Eng. 373-383 (1997); J. Rodolfo, H. Rajbenbach and J-P. Huignard, "Performance of a photorefractive joint transform correlator for fingerprint identification," *Opt. Eng.*, **34**(4), 1166-1171 (1995); Refregier and B. Javidi, "optical Image Encryption using Input and Fourier Plane Random Phase Encoding, " *Opt. Lett.*, **20**, 767-769, (1995); M. Kowalczyk, "Spectral and imaging properties of uniform diffusers", JOSA A, Vol. 1, No. 2, 192-200, February 1984.; H. Kogelnik and K.S. Pennington, "Holographic imaging through a random medium", *Optical Society of America.*, **58**, 2, 273-274, (1968) which are incorporated herein by reference). One approach is to permanently and irretrievably bond an optical key such as a phase mask to a primary identification amplitude pattern, such as a fingerprint, a picture of a face, or a signature. The security system is based on verification of the authenticity of the biometrics information and the phase mask. For additional security, the primary pattern can also be phase encoded. This technique can be applied to verify personal identification and the authenticity of objects

In this invention a new method for optical security verification based on phase encoded convolution of the primary image by a random phase code is proposed. The convolution of the primary image and random mask yields position-invariance to a possible shift of the primary image or the random mask. In this method, a nonlinear joint transform correlator verifies the biometrics information and the random code simultaneously to determine whether or not an object such as an ID card is authentic and that is being used by an authorized person. The binarization of the phase information encoded on the input card is disclosed. Finally, a composite reference image obtained from a set of rotated primary images and convolved with the random code, in order to

obtain position and rotation-invariance is used. It will be appreciated that, this system tolerates rotational variations of the input images. The performance of the proposed method is investigated using a number of metrics. An opto-electronic architecture is proposed to perform the verification. The discrimination capability of the proposed technique against unauthorized codes or unauthorized primary images is investigated in the presence of additive noise and distortions. Finally, the robustness of the proposed method in the presence of noise and distortions such as missing data is addressed.

SUMMARY OF THE INVENTION

A method of verifying the authenticity of an object is presented. The method comprises providing a primary image; providing a secondary image; encoding the primary image; providing a random code; convolving the encoded primary image with the random code, providing thereby a reference image; affixing the reference image to the object to be authenticated; transforming the reference image; and comparing the transformed reference image with the secondary image. A system for verifying the authenticity of an object is presented. The system comprises a signal source; a first subsystem receiving a first signal from the signal source and providing as output therefrom a first output signal; a second subsystem receiving a second signal from the signal source and providing as output therefrom a second output signal; a third subsystem receiving the first and second output signals for comparing the first output signal with the second output signal.

DESCRIPTION OF THE DRAWINGS

Figure 1 is a schematic representation of a system for security verification of an object.

Figure 1A is a schematic representation of an optical setup for security

verification of an object based upon a nonlinear joint transform correlator.

Figure 2 is the fingerprints used in the test: a) is used as an authorized fingerprint. b) is used as an unauthorized fingerprint.

Figure 3 is the nonlinear joint transform correlation results for verification and validation of inputs, with nonlinearity k=0.3. a) out put correlation intensity for the authentic input. b) output for authorized input with unauthorized code. c) output for unauthorized input with authorized code. d) output for unauthorized input and unauthorized code.

Figure 4 is the input primary image fingerprint of Fig. 2(a) corrupted by additive noise. a) zero mean white noise of standard deviation of 0.3. b) zero mean colored noise of standard deviation of 0.3 and bandwidth of 15.

Figure 5 is the simulation results of the system in the presence of additive white noise versus the index nonlinearity k. The results correspond to the white noise on the reference image with standard deviation of 0.7 and different input additive noise levels. The curves designated by an asterisk (*) correspond to the performance of the system in the absence of input noise. a) average of the discrimination ratio (DR) between authorized and unauthorized card with unauthorized fingerprint. b) average of the discrimination ratio (DR) between authorized and unauthorized card with unauthorized code. c) output Signal-To-Noise ration (SNR). d) output Peak-to-Output Energy ratio (POE).

Figure 6 is the simulation results of the system in the presence of additive color noise with bandwidth of 15 versus the k index nonlinearity. The results correspond to the additive color noise on the reference with standard deviation of 0.7 and different input additive color noise levels. The curves designated by an asterisk (*) correspond to the

performance of the system in the absence of input noise. a) average of the discrimination ratio (DR) between authorized and unauthorized card with unauthorized fingerprint. b) average of the discrimination ratio (DR) between authorized and unauthorized card with unauthorized code. c) out put Signal-To-Noise ration (SNR). d) output Peak-to-Output Energy ratio (POE).

Figure 7 is the input primary pattern with missing data when 25% of the authorized fingerprint is blocked.

Figure 8 is the correlation results for verification and validation of cards with nonlinearity k=0.3. The authorized fingerprint has 25% of missing data. a) output correlation intensity for the authentic card. b) output correlation intensity for the authoreized input with unauthorized code. c) output correlation intensity for the unauthorized input with authorized code. d) output correlation intensity for the unauthorized input with unauthorized code.

Figure 9 is the correlation results for discrimination between authorized and unauthorized inputs using the rotation-invariant reference image encoded on the card. a) results for authorized input. b) results for unauthorized input with unauthorized fingerprint. c) results for unauthorized input with unauthorized code. d) results for unauthorized input with unauthorized fingerprint and unauthorized code.

Figure 10 is the binary phase information encoded at input.

Figure 11 is the correlation results for discrimination between authorized and unauthorized cards using the binarization of the reference encoded at the input. a) results for authorized input. b) results for unauthorized input with unauthorized fingerprint. c) results for unauthorized input with unauthorized code. d) results for unauthorized input with unauthorized fingerprint and unauthorized code.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The proposed method for security is based on convolution of the primary image by a random code. The primary image *f(x,y)* is phase encoded, which can be mathematically represented by, *exp[i π f(x,y) / Max(f(x,y))]*. The range of variation of the phase encoding is *[0, π]*. The phase-encoded primary image is convolved by a random code *c(x,y)*. In this invention the random code *c(x,y)* is chosen to be the Fourier transform of a phase only uniform random distribution(8 which is incorporated herein by reference). With this special choice of *c(x,y)* the invention is assured to have high light efficiency output. The resulting convolved image is a complex amplitude distribution:

$$r(x,y) = \exp[i\ \pi f(x,y) / Max(f(x,y))] \otimes c(x,y), \qquad (1)$$

where $\otimes$ denotes convolution.

The convolved image *r(x,y),* will be placed on a card or the object to be verified. It will serve as the reference image to the optical processor. Therefore, the information encoded on the card is a combination of primary information *f(x,y)* and a machine code *c(x,y)*. For additional security, the convolved pattern *r(x,y),* placed on the ID card or any personal document, can be made to be a phase only information by setting the amplitude of the complex distribution *r(x,y)* to one (S. Maze and Ph. Refregier, "Optical correlation: invluence of the coding of the input image" A*ppl. Opt.* **33**, 6788-6796 (1994); S. Maze and Ph. Refregier, "Noise robustness of optical correlation for amplitude or phase modulationof the input image", *Opt. Lett.*, **17**, 426-428, (1992) which are incorporated herein by reference). The phase only pattern reference image on the ID card or on the personal document is given by

$$\bar{r}(x,y) = \frac{r(x,y)}{|r(x,y|}. \qquad (2)$$

This invention will also investigate the performance of binarization of the phase information of the reference encoded on the document. The binarization of the reference image is given by:

$$\overline{r_B}(x,y) = \begin{Bmatrix} -1 \; if \; \mathrm{Re}[r(x,y)] < 0, \\ 1 \; if \; \mathrm{Re}[r(x,y)] \geq 0, \end{Bmatrix} \tag{3}$$

where Re[*r(x,y)*] is the real part of *r*(*x*,y). (C.J. Weaver and J. W. Goodman, "A technique for optically convolving two functions" *Appl. Opt.* **5,** 1248-1249 (1966).

A joint transform correlator (JTC) architecture which is incorporated herein by reference) is used to verify the authenticity of the card. A nonlinear JTC is more practical because of the limited dynamic range of optical devices. In addition, the nonlinear JTC offers many advantage in terms of correlation performance(B. Javidi, "Nonlinear joint transform correlators," in *Real-Time Optical Information Processing,* B Javidi and J.L. Horner, Eds., Academic Press, New York, (1994); B. Javidi, "Nonlinear joint power spectrum based optical correlation," *Appl. Opt. 28,* 2358- 2367 (1989) which are incorporated herein by reference). A nonlinear joint transform correlator is used to perform the correlation between the convolution of the phase encoded primary pattern and the random code mask and the phase distribution, recorded on the card given by equation 2. In the Fourier plane of the nonlinear joint transform correlator, we use a threshold function which is the sum of the self-product terms of the joint power spectrum. A k-th-power-law nonlinearity ($0 \leq k \leq 1$) is applied to the modified joint power spectrum in the Fourier plane(B. Javidi, "Nonlinear joint transform correlators," in *Real-Time Optical*

Information Processing, B Javidi and J.L. Horner, Eds., Academic Press, New York, (1994); B. Javidi, "Nonlinear joint power spectrum based optical correlation," *Appl. Opt. 28,* 2358- 2367 (1989) which are incorporated herein by reference). An inverse Fourier transform of the nonlinearly transformed joint power spectrum will generate the nonlinear joint transform correlator output plane. If $s(x,y)$ is the signal to be verified, the nonlinear joint transform correlator output of our system is given by

$$Output(x,y) = s(x,y) *^{k} \bar{r}(x,y) \qquad (4)$$

where the superscript $(*k)$ denotes the k-th law nonlinear joint transform correlation, and k∈[0,1] is the severity of the nonlinearity used in the Fourier plane(w B. Javidi, "Nonlinear joint transform correlators," in *Real-Time Optical Information Processing,* B Javidi and J.L. Horner, Eds., Academic Press, New York, (1994); B. Javidi, "Nonlinear joint power spectrum based optical correlation," *Appl. Opt. 28,* 2358- 2367 (1989) which are incorporated herein by reference). The k-th law nonlinear JTC in the Fourier plane is defined by: $|RS|^{k} exp[j\phi_{s} - j\phi_{R}]$, where $|R|exp[j\phi_{R}]$ and $|S|exp[j\phi_{s}]$ are the Fourier transforms of the reference image and the input image, respectively. When the phase of the reference input is binarized, the k-th law nonlinear joint transform correlator output is define as

$$Output(x,y) = s(x,y) *^{k} \bar{r}_{B}(x,y) \qquad (5)$$

OPTICAL SET-UP DESCRIPTION

In Fig. 1 a schematic representation of a system for security verification is shown generally at 700. In particular in Fig. 1 a source of coherent light 100 is provided to illuminate 102 first and second Fourier transform optical subsystems 200, 300. The first Fourier transform optical subsystem 200 provides as output therefrom a first optical output signal 206 indicative of the Fourier transform of the convolution of the random code, $c(x,y)$, and the phase encoded primary image, $\exp\{i\pi f(x,y)/\mathrm{Max}[f(x,y)]\}$. The second Fourier transform optical subsystem 300 provides as output therefrom a second optical output signal 312 indicative of the Fourier transform of the a phase only convolved image, $\bar{r}(x',y')$. The first and second optical output signals 206, 312 are detected at a detector 400. A signal 402 indicative of the joint power spectrum of the first and second optical signals 206, 312 is provided as output from the detector 400 to a verification subsystem 500 for correlation thereof.

The optical setup for security verification 700 is shown in Fig. 1A as a nonlinear joint transform correlator (JTC) 700. The optical system700 consists of two arms. In one arm, the convolution of a secondary image such as the phase encoded primary pattern $\exp\{i\pi f(x,y)/Max[f(x,y)]\}$ and the random code, $c(x,y)$, is performed by use of a spatial filter matched to the random code $c(x,y)$, and positioned in the Fourier or (u,v) plane. The phase-encoded primary pattern is displayed by means of a spatial light modulator (SLM) 208. Fourier transform lens L_1 210, images the Fourier transform (FT) of the phase-encoded primary pattern, $F(u,v)$, in the Fourier, or (u,v), plane. The processor 700 has an *a-priori* knowledge of the random code mask $c(x,y)$. Thus, in the (u,v)-plane, a filter 212 with transmission $C(u,v)$ is the Fourier transform of the random code $c(x,y)$. Lenses L_2 and L_3 214, 216, image the complex amplitude distribution formed at the filter plane on the (α,β)-plane, where a detector 400 is placed. Thus the Fourier transform of the convolution between the two functions $exp[i\,\pi f(x,y)\,/\,Max(f(x,y))]$ and $c(x,y)$ is obtained

in (α,β)-plane. In the other arm, an object, whose authenticity is to be verified and including a reference image such as the phase only distribution, $\bar{r}(x',y')$, is placed in the input plane (x',y') of the processor 700. Coherent light 308 illuminates the reference image 602. Lens L_4 306 images the Fourier transform of $\bar{r}(x',y')$ on the (α,β)-plane of the detector 400. Thus, a joint power spectrum is obtained in (α,β)-plane. The joint transform interference intensity is recorded by the detector 400 and is nonlinearly transformed by a nonlinear transfer function generator 502 in the verification subsystem 500. The resulting modified joint transform spectrum is inverse Fourier transformed and the modulus thereof squared to obtain the correlation. The correlation signal may be obtained either by performing optical Fourier transform by displaying the modified intensity distribution written on the SLM, or by using discrete Fourier transform.

It will be appreciated to one skilled in the art that the aforedescribed system for verifying the authenticity of an object is not limited to an optical system but also encompasses electronic systems as well as combinations thereof. It will also be appreciated that the signals generated therein may be either one dimensional or two dimensional or *n* dimensional.

COMPUTER SIMULATION RESULTS

Computer simulations have been conducted to investigate the performance of the proposed optical systems.

In the simulations, a discrimination capability of the security system against an unauthorized input card is examined. The card is considered to be unauthorized, when either the input primary biometrics image or the random code is unauthorized. To evaluate the discrimination, we define the discrimination ratio (DR) as

$$DR = \frac{\left|\max[AC(x,y)]\right|^2}{\left|\max[CC(x,y)]\right|^2}, \qquad (6)$$

where max [AC(x,y)] is the auto-correlation peak value, and max [CC(x,y)] is the maximum value of the cross-correlation output. The auto-correlation is defined as

$$AC(x,y) = \left[\exp[\, i\,\pi\ f(x,y)\ /\ \mathrm{Max}(f(x,y))] \otimes c(x,y)\right]^{*k}\left(\frac{\exp[i\,\pi\ f(x,y)\ /\ \mathrm{Max}\,(f(x,y))] \otimes c(x,y)}{\exp[i\pi\ f(x,y)\ /\ \mathrm{Max}\,(f(x,y))] \otimes c(x,y)}\right)$$

(7)

where *f(x,y)* is the authorized primary pattern and *c(x,y)* is the authorized code as defined in Section (2). The cross-correlation is defined as:

$$CC(x,y) = \left[\exp\,[\, i\,\pi\ g(x,y)\ /\ \mathrm{Max}(g(x,y))] \otimes a(x,y)\right]^{*k}\left(\frac{\exp[i\,\pi\ f(x,y)\ /\ \mathrm{Max}(f(x,y))] \otimes c(x,Y)}{\exp[i\,\pi\ f(x,y)\ /\ \mathrm{Max}(f(x,y))] \otimes c(x,y)}\right)$$

(8)

where *g(x,y)* is an unauthorized primary pattern and/or *a(x,y)* is an unauthorized code. The higher the DR, the better the discrimination of the system is against unauthorized inputs.

In addition, the robustness of the proposed optical security system in the presence of additive input noise is investigated. In the noise performance tests of the system, both

white and color noise are considered. The performance of the proposed method is investigated using a number of metrics. The signal to noise ratio SNR is defined as the ratio of the expected value squared of the correlation peak amplitude to the variance of the correlation peak amplitude. And the peak-to-output energy ration metric POE is defined as the ratio of the expected value squared of the correlation peak to the average expected value of the output signal energy.

DISCRIMINATION CAPABILITY

Throughout the simulations, fingerprint biometrics are used as the primary image; however the other biometrics can be used as well. The optical processor was first tested for authenticity of a card encoded with a fingerprint information convolved with a random code in the absence of input noise and distortions. Two fingerprints are selected for computer simulation as shown in Figure 2. The fingerprint in Figure 2(a) is chosen as the authentic and the fingerprint in Figure 2(b) is considered as an unauthorized biometric image to be rejected. Figure 3(a) is the output correlation intensity for the authentic card, when the authorized fingerprint and code are used. A sharp and strong output peak for the authentic card is obtained. The simulations in Figure 3 were done with nonlinearity index of k=0.3 for the correlator. In the experiments, the correlation output are normalized by the maximum correlation peak obtained by the authentic card. Figures 3 (b), 3 (c) and 3 (d) show the output correlation intensity for the false class input, where very low level cross-correlations appear. Figure 3(b) shows the outputs correlation for an authorized fingerprint and an unauthorized random code. Figure 3(c) shows the correlation output for the authorized random code and an unauthorized fingerprint. Figure 3(d) shows the output correlation plane for an unauthorized fingerprint and an unauthorized code.

ROBUSTNESS TO INPUT NOISE AND DISTORTION

The correlation output of the proposed processor is investigated in the presence of input noise or other distortions such as missing data in order to study the robustness of the system. To test the noise tolerance of this method, we consider different kinds of additive noise. The reference to be verified may contain some surface noise, due to continuous use. Also, during the real time registration of the primary pattern for verification, the detector may introduce some noise which we will consider in the simulations. The output of the nonlinear joint transform correlator in the presence of additive noise can be written as

$$\text{Output}(x,y) = \left\{\exp\left[i\pi\left(f(x,y) + n_p(x,y)\right)/\text{Max}\left(f(x,y) + n_p(x,y)\right)\right] \otimes c(x,y)\right\}^{*k}$$
$$\left\{\frac{\exp\left[i\pi\left(f(x,y)\right)/\text{Max}\left(f(x,y)\right)\right] \otimes c(x,y)}{\left|\exp\left[i\pi\left(f(x,y)\right)/\text{Max}\left(f(x,y)\right)\right] \otimes c(x,y)\right| + n_c(x,y)}\right\}, \quad (9)$$

where $n_p(x,y)$ and $n_c(x,y)$ are the additive noise present on the primary image and, the card, respectively.

Simulation results are presented to illustrate the robustness of the system against additive noise using a k-th law nonlinear JTC. The signal to noise ratio (SNR), discrimination ratio (DR), and peak-to-output energy ratio (POE) are measured. The simulation of the input noise on the input card and on the reference image has been carried out for several values of standard deviation. The performance parameters are computed for 50 different sample realizations of the input signals corrupted by noise.

The experiments were conducted with both additive white noise and color noise. In the simulations, a range of values for the nonlinearity index k of the correlator has been tested. The input biometrics was corrupted by Gaussian noise, with standard deviation of 0.1, 0.2 and 0.3 Figure 4(a) shows the noisy image with white noise of standard deviation 0.3. In the simulations, the reference encoded on the card is also corrupted by a zero mean additive white noise with standard deviations of 0.3, 0.5 and 0.7. The noise robustness variation results obtained are similar for all three levels of noise that corrupt the information encoded on the card. Here, we present the results obtained with a noise level standard deviation of 0.7. The experiment was done by simulating 50 realizations of white noise.

Figure 5(a) and 5(b) show the variation of the discrimination ratio (DR) versus the nonlinearity index k of the correlator, when the primary pattern is corrupted by additive Gaussian white noise with different standard deviations. Fig. 5(a) corresponds to the discrimination against unauthorized input card with an authentic code and an unauthorized fingerprint. Fig 5(b) corresponds to the discrimination against unauthorized input card encoded with an unauthorized code and an authentic fingerprint.

Figure 5(c) and 5(d) illustrate the SNR and the POE as function of the nonlinearity k when the primary pattern is corrupted by additive Gaussian white noise with different standard deviations.

The experiments were repeated with the biometrics images that were corrupted by zero mean additive color noise of bandwidth equal to 15, and various standard deviations. Figure 4(b) shows the corrupted image with additive color noise with standard deviation of 0.3 and bandwidth of 15. In the simulations, the encoded reference on the card is also corrupted by a zero mean additive color noise with bandwidth of 15 and standard deviation of 0.3, 0.5 and 0.7. The results obtained for the reference corrupted with an

additive color noise of standard deviation 0.7 are presented. The experiment was done over the results of 50 realizations of independent noise.

Figures 6(a) through 6(d) illustrate the performance of the processor versus the nonlinearity index k in presence of the additive color noise, in terms of DR, SNR and POE, respectively. Figures 6(a) and 6(b) correspond to the false class inputs with an unauthorized fingerprint and an unauthorized code, respectively.

The robustness to missing data during the acquisition of the primary pattern information is tested. Figure 7 shows an example of input primary pattern with missing data when 25% of the authorized fingerprint is blocked. The tests with missing input data are presented in Figure 8. In the simulation presented here, additive white noise used for both the input primary pattern (with standard deviation of 0.3) and for the reference encoded on the credit card (with standard deviation of 0.7).

VALIDATION AND VERIFICATION USING ROTATIONS-INVARIANT ENCODED REFERENCES

System performance using rotation-invariant encoded references is disclosed. In real applications of the system, rotation of the primary pattern during the acquisition process of the fingerprint may occur. Some simulation of in-plane rotation indicate that, the system proposed in this paper can tolerate one degree of input image rotation. The sensitivity depends on the nonlinearity index k. The smaller the nonlinearity index k, the more sensitive the system is to rotation changes in input primary pattern. The range of the rotation of the primary pattern during the acquisition process may be very limited, and it can be reduced by the system, using a guide for the user's finger: thus a controlled environment may be used.

To improve the rotation robustness of the system, we develop a rotation invariant

primary pattern using a training set of rotated images. The rotation invariant primary pattern is encoded on the card. This rotation invariant primary pattern is a linear combination of several images of a single fingerprint. Each image is rotated by a small angle. The rotation-invariant pattern encoded on the card is given by the following equation,

$$\bar{p}(x,y) = \frac{\left\{\sum_a \exp[i\pi\, f_a(x,y) / \mathrm{Max}(f_a(x,y))]\right\} \otimes c(x,y)}{\left|\left\{\sum_a \exp[i\pi\, f_a(x,y) / \mathrm{Max}(f_a(x,y))]\right\} \otimes c(x,y)\right|} \qquad (10)$$

where $f_a(x,y)$ is the primary pattern rotated by an angle α. In the experiment presented here the sum is over -10 to +10 degrees with increments of 1 degree, and the rotation axis coincides with the center of the image. The correlation results correspond to nonlinear JTC for k=0.3 Fig. 9(A) is the output correlation intensity for the authentic input card, using a rotation-invariant reference image encoded on the card. Here the correct fingerprint is rotated by 7 degrees and the authorized code is used. A sharp and strong output peak is obtained Figs. 9(b), (c) and (d) show the output correlation intensity for false inputs, where no correlation peak appears. In the simulation presented here , additive white noise is taken into account for forth the input primary pattern (with standard deviation of 0.3) and for the reference encoded on the card (with standard deviation of 0.7). In the experiments, the correlation output are normalized by the maximum correlation peak obtained by the authentic card. Fig. 9(b) shows the correlation

output for an authorized random code and an unauthorized fingerprint. Fig. 9(c) shows the output correlation for an authorized fingerprint and an unauthorized random code. Fig. 9(d) shows the output correlation plane for an unauthorized fingerpring and an unauthorized code. The tests illustrate that the rotation invariant reference image provides tolerances to rotation of input primary images.

BINARIZATION OF THE REFERENCE ENCODED ON THE CARD

The system performance when the phase information encoded on the card is binarized is disclosed. Display of the complex spatial distribution on the card may not be trivial. To remedy this problem, we test the binarization of the distribution which is to be encoded on the card. The reference image encoded on the card at each point is set to 1 when the real part of the reference image is positive and to -1 otherwise [see Eq. (3)]. This approach leads to a 2-D binary pattern placed on the card. It is shown that in the simulation, the verification and the validation are obtained with high accuracy. Figure 10 illustrates the binary phase distribution encoded on the card obtained by using Eq. 3.

Figure 11(a) is the output correlation intensity for the authentic card. Figs. 11(b), (c) and (d) show the output correlation intensity for an unauthorized card where no correlation peak appears. Fig. 11(b) shows the correlation output for an authorized random code and an unauthorized fingerprint. Fig. 11(c) shows the output correlation for an authorized fingerprint and an unauthorized random code. Fig 11(d) shows the output correlation plane for an unauthorized fingerprint and an unauthorized code. Binarization of the information on the card in the proposed system can provide good discrimination ratio for verification and validation.

CONCLUSIONS

A new method for security verification of objects such as card, using optical

pattern recognition is proposed. This method is based on phase encoded convolution of the primary pattern with a random code placed on the card. An optical system to perform the verification has been described. The correlation is performed using the nonlinear JTC. For the images presented here, the proposed method can identify an authorized input by producing well defined output peaks, and it rejects the unauthorized input with high discrimination ratio. The performance of the system in terms of input noise, biometric rotation, and missing data has been investigated. For the tests provided here, the proposed system is found to be robust to noise added to input primary pattern and to the reference pattern encoded on the card. The nonlinear correlation allows a compromise between the noise tolerance and the discrimination ratio. The tests using missing data show that, for the fingerprint image used in the simulation, the system provides good tolerance up to 25% of missing data in the input primary pattern and that the security verification of the authorized input is highly discriminate against the unauthorized inputs. The rotation invariant composite reference primary pattern is designed to provide tolerance to rotation of the input primary image. Binarization of the phase information encoded on the card has been tested. The results indicate that the verification is obtained with high discrimination ratio of authorized inputs against unauthorized inputs.

Various kinds of optical data processing technology for information security have been proposed. (H.-Y.S. Li, Y. Qiao, and D. Psaltis, Appl. Opt. 32, 5026 (1993); B. Javidi and J.L. Horner, Opt. Eng. 33, 1752 (1994); P. Refregier and B. Javidi, Opt. Lett. 20, 767 (1995); F. Goudail, F. Bollaro, B. Javidi, and P. Refregier, J. Opt. Soc. Am. A15, 2629 (1998); C.L. Wilson, C. I. Watson, and E.G. Paek, Proc. SPIE 3078, 373 (1997); D. Weber and J. Trolinger, Opt. Eng. 38, 62 (1999); O. Matoba and B. Javidi, Opt. Lett. 24, 762 (1999), all of which are incorporated herein by reference). In one approach (P. Refregier and B. Javidi, Opt. Lett. 20, 767 (1995), which is incorporated herein by

reference), the data are encrypted optically by double-random phase encoding with uniformly distributed random phase keys in both the input and Fourier planes. In addition, digital holographic techniques (U. Schnars and W. Juptner, Appl. Opt. 33, 179 (1994); I. Yamaguchi and T. Zhang, Opt. Lett. 22, 1506 (1997); E. Cuche, F. Bevilacqus, and C. Depeursinge, Opt. Lett. 24, 291 (1999), which are incorporated herein by reference) that use a CCD camera for direct recording of a hologram have become available owing to the development of the imaging technology.

In this invention a security system that combines double-random phase encryption with a digital holographic technique is proposed. The proposed system enables us to store, transmit, and decrypt the encrypted data digitally. One benefit of the proposed system compared with electronic encryption techniques is that optical processing provides many degrees of freedom for securing information. Another benefit is that optical encryption is naturally suited to encrypting information, e.g., real images and information stored in holographic media, that exists in the optical domain. Either optical or computer decryption techniques can be used with the proposed system, depending on the specific application. Computer decryption is less secure because the phase key is stored electronically, but no manual focusing adjustment is required and the decryption system is more compact.

12

Figure 11 shows the secure image/video-storage/transmission system based on the proposed system. The data are encrypted optically by the double-random phase encryption technique and recorded as a digital hologram. The optical key, that is, the Fourier phase mask, can also be recorded as a digital hologram. The encrypted data can be decrypted digitally with the hologram of the optical key.

Let $f(x,y)$, $a(x,y)$, and $H(\xi,\eta)$ denote the image to be encrypted, the input random phase mask, and the Fourier random phase mask, respectively. The input random phase

mask, $a(x,y)$, is bonded with the image $f(x, y)$. The resultant product of the two images is Fourier transformed and is multiplied by the Fourier phase mask $H(\xi, \eta)$. A second Fourier transform products the encrypted data. We record the encrypted data as a Fourier hologram, using and interference with the reference wave $R(\xi, \eta)$. The hologram $Ig(\xi, \eta)$ can be written as

$$I_E(\xi, \eta) = |[F(\xi, \eta) \otimes A(\xi, \eta)]H(\xi, \eta)|^2 + |R(\xi, \eta)|^2$$
$$+ \{[F(\xi, \eta) \otimes A(\xi, \eta)]H(\xi, \eta)\}R(\xi, \eta)^*$$
$$+ \{[F(\xi, \eta) \otimes A(\xi, \eta)]H(\xi, \eta)\}^* R(\xi, \eta),$$

where $F(\xi, \eta)$ and $A(\xi, \eta)$ denote Fourier transforms of $f(x,y)$ and $a(x,y)$, respectively, and $\otimes$ denotes a convolution operation. Inasmuch as we can know the first and second terms on the right-hand side of Eq. (11) *a priori* by obtaining the power spectrum of the encrypted data and reference beam, we can get the following holographic data, $I_{E'}(\xi, \eta)$:

$$I_E'(\xi, \eta) = \{[F(\xi, \eta) \otimes A(\xi, \eta)]H(\xi, \eta)\}R(\xi, \eta)^*$$
$$+ \{[F(\xi, \eta) \otimes A(\xi, \eta)]H(\xi, \eta)\}^* R(\xi, \eta).$$

Similarly, we can also obtain the holographic data of the Fourier phase mask, $I_{M'}(\xi, \eta)$ given by $$I_M'(\xi, \eta) = H(\xi, \eta)R(\xi, \eta)^* + H(\xi, \eta)^* R(\xi, \eta).$$

When the reference beam is a slightly inclined planar wave, we can extract the first term on the right-hand side of Eq. (12) and the second term on the right-hand side of Eq. (13) by Fourier transforming the holographic data to obtain the encrypted data and the Fourier phase mask, respectively. By multiplying the extracted encrypted data and the Fourier phase mask followed by inverse Fourier transformation, we can obtain the decrypted data, $d(x,y)$ as

$$\begin{aligned} d(x, y) &= \mathrm{FT}^{-1}[(\{[F(\xi, \eta) \circledast A(\xi, \eta)]H(\xi, \eta)\}R(\xi, \eta)^*) \\ &\quad \times [H(\xi, \eta)^* R(\xi, \eta)]] \\ &= \mathrm{FT}^{-1}[F(\xi, \eta) \circledast A(\xi, \eta)] \\ &= f(x, y)a(x, y), \end{aligned}$$

where FT^{-1} [] denotes the inverse Fourier transform operation and $|H(\xi,\eta)|^2$ is equal to a constant because the phase mask has only phase value. The intensity of Eq. (14) produces the original image because $f(x,y)$ is a positive real-valued function and $a(x,y)$ is phase only.

The experimental system is shown in Fig. 12. It consists of a Mach-Zehnder interferometer. A He-Ne laser is used as a coherent light source. The lower arm of the interferometer is the optical path of the image encryption. The upper arm is the reference wave. The input image to be encrypted is bonded with the input phase mask at plane P1. This product is Fourier transformed by lens L1 and is multiplied by the Fourier phase mask at plane P2 and imaged onto the CCD camera by the 4-f optical system of lenses L2 and L3. The reference wave passes through the 4-f optical system of lenses L4 and L5 to

keep the spatial coherence.

At the CCD camera, a hologram is created by the interference between the encrypted data and the slightly inclined reference plane wave. The hologram captured by the CCD camera is sampled with 512 X 480 pixels and is quantized to 8 bits of gray levels by means of the frame-grabber board. The input image, the input phase mask, and the lens L1 are removed when we record the hologram of the Fourier phase mask. In the experiments, we use a random phase mask with a correlation length of less than 10μm as an input phase mask and a lens as the Fourier phase mask.

The reason why we use a lens is the lack of sufficient space-bandwidth product of both the optical system and CCD camera to permit us to employ a wide-angle random phase make with a small correlation length of less than10μm. To remedy this problem, phase masks can be designed to take into account the available space-bandwidth product of the optical system. Lens L1 has a numerical aperture of 0.10, lenses L2 and L3 each have a numerical aperture of 0.14, and lenses L4 and L5 each have a numerical aperture of 0.17. The CCD array has dimensions 6.4 x 4.8mm.

Figure 13 shows the input images to be decrypted. These electronically reconstructed images are obtained with an input phase mask without the Fourier phase mask. Scattering that is due to the thickness of the input random phase mask and the limitation on the numerical aperture of the lens L1 are the reasons why the images are somewhat noisy.

Digital holograms of the encrypted data and the Fourier phase mask are shown in Fig.1 4. The digitally reconstructed encrypted images are shown in Fig. 15. These images were obtained by inverse Fourier transforming of the digital hologram of the encrypted data. The original images cannot be recognized. The mean-square errors between the original images MEMORY and UCONN and the encrypted images are 7.3

and 6.6, respectively. The digitally reconstructed images that have been decrypted with the hologram of the Fourier phase mask are shown in Fig. 16. Here one can see the original images. The mean-square errors between the original images MEMORY and UCONN and the decrypted images are 0.97 and 1.1, respectively. The experimental results demonstrate the feasibility of the proposed method.

In conclusion, we have presented an image security method that uses digital holography. This method allows the encrypted data to be stored, transmitted, and decrypted digitally. Optical experiments has been shown to illustrate the proposed method. The system can be used for secure video storage and transmission.

Optical data processing technology for information security have been proposed . (H.-Y.S. Li, Y. Qiao, and D. Psaltis, Appl. Opt. 32, 5026 (1993); B. Javidi and J.L. Horner, Opt. Eng. 33, 1752 (1994); P. Refregier and B. Javidi, Opt. Lett. 20, 767 (1995); F. Goudail, F. Bollaro, B. Javidi, and P. Refregier, J. Opt. Soc. Am. A15, 2629 (1998); C.L. Wilson, C. I. Watson, and E.G. Paek, Proc. SPIE 3078, 373 (1997); D. Weber and J. Trolinger, Opt. Eng. 38, 62 (1999); O. Matoba and B. Javidi, Opt. Lett. 24, 762 (1999), all of which are incorporated herein by reference). In one approach , (P. Refregier and B. Javidi, Opt. Lett. 20, 767 (1995), which is incorporated herein by reference) he data is encrypted optically by double random phase encoding using uniformly distributed random phase keys in both the input and Fourier planes. In addition, digital holographic techniques w (U. Schnars and W. Juptner, Appl. Opt. 33, 179 (1994); I. Yamaguchi and T. Zhang, Opt. Lett. 22, 1506 (1997); E. Cuche, F. Bevilacqus, and C. Depeursinge, Opt. Lett. 24, 291 (1999), which are incorporated herein by reference) hich use a CCD camera for direct recording of a hologram have been available owing to the development of the imaging technology.

In this Letter, we propose a security system that combines the double random

phase encryption and the digital holographic technique. The proposed system enables us to store, transmit, and decrypt the encrypted data digitally. Figure 11 shows the secure image/video strage/transmission system based on the proposed system. The data is encrypted optically using the double random phase encryption and is recorded as a digital hologram. The optical key, that is, the Fourier phase mask is also recorded as a digital hologram. The encrypted data is decrypted digitally by using the hologram of the optical key.

Let $f(x,y)$, $a(x,y)$, and $H(\xi,\eta)$ denote the image to be encrypted, the input random phase mask, and the Fourier random phase mask, respectively. The input random phase mask $a(x,y)$, is bonded with the image $f(x,y)$. This resulting product of the two images is Fourier transformed and is multiplied with the Fourier phase mask $H(\xi,\eta)$. A second Fourier transform produces the encrypted data. We record the encrypted data as a Fourier hologram using an interference with the reference wave $R(\xi,\eta)$. The hologram $I_E(\xi,\eta)$ can be written as

$$I_E(\xi,\eta) = \left|\left[F(\xi,\eta)\otimes A(\xi,\eta)\right]H(\xi,\eta)\right|^2 + \left|R(\xi,\eta)\right|^2$$
$$+\left[\left[F(\xi,\eta)\otimes A(\xi,\eta)\right]H(\xi,\eta)\right]R(\xi,\eta)^* + \left[\left[F(\xi,\eta)\otimes A(\xi,\eta)\right]H(\xi,\eta)\right]^* R(\xi,\eta),$$

where $F(\xi,\eta)$ and $A(\xi,\eta)$ denote Fourier transforms of $f(x,y)$ and $a(x,y)$, respectively. The notation $\otimes$ denotes convolution operation. Since the first and second terms on the right-hand side of Eq. (15) can be known a priori by obtaining the power spectrum of the encrypted data and reference beam, we can get the following holographic data, $I'_E(\xi,\eta)$:

$$I'_E(\xi,\eta) = \left[\left[F(\xi,\eta)\otimes A(\xi,\eta)\right]H(\xi,\eta)\right]R(\xi,\eta)^* + \left[\left[F(\xi,\eta)\otimes A(\xi,\eta)\right]H(\xi,\eta)\right]^* R(\xi,\eta).$$

Similarly, we can also obtain the holographic data of the Fourier phase mask, $I_M(\xi,\eta)$, given by

$$\Gamma_M(\xi,\eta) = H(\xi,\eta)R(\xi,\eta)^* + H(\xi,\eta)^* R(\xi,\eta).$$

When the reference beam is a slightly inclined planar wave, we can extract the first term on the right-hand side of Eq. (16) and the second term on the right-hand side of Eq. (17) by Fourier transforming the holographic data to obtain the encrypted data and the Fourier phase mask, respectively. By multiplying the extracted encrypted data and the Fourier phase mask followed by inverse Fourier transformation, the decrypted data *d(x,y)* can be obtained as

$$\begin{aligned} d(x,y) &= FT^{-1}\Big[\Big[\Big[\big[F(\xi,\eta)\otimes A(\xi,\eta)\big]H(\xi,\eta)\Big]R(\xi,\eta)^*\Big]\cdot\Big[H(\xi,\eta)^* R(\xi,\eta)\Big]\Big] \\ &= FT^{-1}\big[F(\xi,\eta)\otimes A(\xi,\eta)\big] \\ &= f(x,y)\alpha(x,y), \end{aligned}$$

where $FT^{-1}[\ ]$ denotes the inverse Fourier transform operation and $H(\xi,\eta)^2$ is equal to a constant because the phase mask has only phase value. The intensity of this equation produces the original image because *f(x,y)* is a positive real-valued function and *a(x,y)* is phase only.

The experimental system is shown in Fig. 12. It consists of a Mach-Zehnder

interferometer. He-Ne laser is used as a coherent light source. The lower arm of the interferometer is the optical path of the image encryption. The upper arm is the reference wave. The input image to be encrypted is bonded with the input phase mask at plane P1. This product is Fourier or Fresnel transformed by lens L1 and is multiplied by the Fourier or Fresnel phase mask at plane P2 and imaged on the CCD camera by the 4-f optical system of lenses L2 and L3. The reference wave passes through the 4-f optical system of lenses L4 and L5 in order to keep the spatial coherence. At the CCD camera, a hologram is created by the interference between the encrypted data and the slightly inclined reference plane wave. The hologram captured by CCD camera is sampled with 512 x 480 pixels and is quantized to 8 bits of gray levels via the frame-grabber board. The input image, the input phase mask, and the lens L1 are taken out when we record the hologram of the Fourier or Fresnel phase mask. In the experiments, we use a random phase mask with correlation length of less than10 um as an input phase mask and a lens as the Fourier or Fresnel phase mask. The reason why we use a lens is the lack of sufficient space bandwidth product of both the optical system and the CCD camera to employ a wide angle random phase code with small correlation length of less than 10 um.

Figure 13 shows the input images to be decrypted. These electrically reconstructed images are obtained with an input phase mask without the Fourier or Fresnel phase mask. Scattering due to the thickness of the input random phase mask and the limitation on the numerical aperture of the lens L1 are the reasons why the images are somewhat noisy. The digital hologram of the encrypted data and the Fourier or Fresnel phase mask are shown in Fig. 14. The digitally reconstructed encrypted images are shown in Fig. 15. The image is obtained by inverse Fourier or Fresnel transforming of the digital hologram of the encrypted data. The original image cannot be recognized. The mean square error between the original images "MEMORY" and "UCONN" and the encrypted images are 7.3 and 6.6, respectively. The digitally reconstructed decrypted

images using the hologram of the Fourier phase mask are shown in Fig. 6. Here one can see the original images. The mean square error between the original images "MEMORY and "UCONN" and the decrypted images are 0.97 and 1.1, respectively. The experimental results demonstrate the feasibility of the proposed method.

In conclusion we have presented an image security method using a digital holographic technique. By using this method the encrypted data can be stored, transmitted, and decrypted digitally. Optical experiments have been shown to illustrate our proposed method.

The following references are incorporated herein in their entirety:

1. R.O. Duda, P.E. Hart

Pattern classification and scene analysis

J. lWiley and Sons, 1973

2. R. Schalkoff

Pattern Recognition Statistical, Structural and Neural Approaches

J.Wiley and Sons 1992

3. P. Hariharan

Optical Holography Principles Techniques and Approaches

Cambridge University Press 1984

4. W.H. Lee

Computer Generated Holagraphy, Teniques and Applications

Progress in Optics, Vol 16

Ed., E. Wolf

Amsterdam North Holland 1978

5. J.W. Goodman

Introduction to Fourier Optics

McGraw-Hill 1996